Sur la classification de quelques phi-modules simples

Xavier Caruso

Sur la classification de quelques ϕ-modules simples

Xavier Caruso

Juillet 2008

Dans cet appendice, on détermine les ϕ-modules étales simples sur $\bar{F}_p((u))$ dans une situation légèrement plus générale que celle étudiée dans l'article ([1]). On fixe p un nombre premier et on pose $k = \bar{\mathbb{F}}_p$ et pour tout q, puissance de p, on définit $\mathbb{F}_q$ comme l'unique sous-corps de k de cardinal q. Soit σ un automorphisme de k.et $b > 1$ un entier. On note ℓ le sous-corps de k fixe par σ et, plus généralement, pour tout entier d, on note ℓ_d le sous-corps fixe par σ^d. On considère le corps $K = k((u))$ que l'on munit de l'endomorphisme :

$$\phi\left(\sum_{n=-\infty}^{\infty} a_n u^n\right) = \sum_{n=-\infty}^{\infty} \sigma(a_n) u^{bn}.$$

(Si $b = p$ et $\sigma = \mathrm{id}$, on retrouve donc la situation de l'article.)

On considère la catégorie $\mathrm{Mod}^{\phi}_{/K}$ dont les objets sur les K-espaces vectoriels D de dimension finie muni d'un endomorphisme ϕ-semi-linéaire $\phi_D : D \to D$ dont l'image contient une base de D. Par la suite, lorsque cela ne prêtera pas à confusion, nous noterons simplement ϕ à la place de ϕ_D. Les morphismes de $\mathrm{Mod}^{\phi}_{/K}$ sont bien entendu les applications K-linéaires qui commutent à ϕ. On vérifie aisément que la catégorie $\mathrm{Mod}^{\phi}_{/K}$ est abélienne et que chaque objet est de longueur finie. Le but de cette appendice est de déterminer les objets simples de $\mathrm{Mod}^{\phi}_{/K}$.

Les objets $D(d, n, a)$ et $D(r, a)$

Soient d un entier strictement positif, n un entier naturel et a un élément non nul de k. À ces données, on associe un objet de $\mathrm{Mod}^{\phi}_{/K}$ noté $D(d, n, a)$ défini comme suit :

- $D(d, n) = Ke_0 \oplus Ke_1 \oplus \cdots \oplus Ke_{d-1}$;
- $\phi(e_i) = e_{i+1}$ pour $i \in \{0, \ldots, d-2\}$.
- $\phi(e_{d-1}) = au^n e_0$.

On définit également $D(d, n) = D(d, n, 1)$.

On commence par déterminer des familles d'isomorphismes entre les différents $D(d, n, a)$.

Lemme 1. *Si σ n'est pas l'identité, alors $D(d, n, a)$ est isomorphe à $D(d, n)$ pour tous d, n et a comme précédemment.*

Démonstration. Considérons un élément $\lambda \in k$ tel que $a = \frac{\sigma^d(\lambda)}{\lambda}$ (l'existence résulte d'un théorème classique de théorie de Galois). L'isomorphisme $D(d, n, a) \to D(d, n)$ est alors donné par $e_i \mapsto \sigma^i(\lambda) e_i$. $\square$

Lemme 2. *Soient (d, n, a) et (d, n', a') deux triplets comme précédemment avec le même d. On suppose qu'il existe un entier naturel s tel que $n \equiv b^s n' \pmod{b^d - 1}$ et $a = \sigma^s(a')$. Alors $D(d, n, a) \simeq D(d, n', a')$.*

Démonstration. Si $m = \frac{n - b^s n'}{b^d - 1} \in \mathbb{Z}$, et si $e_0, \ldots, e_{d-1}$ (resp. $e'_0, \ldots, e'_{d-1}$) est la base fournie par la définition, alors un isomorphisme est $e_i \mapsto u^{b^i m} e'_{i+s}$ où les e'_j pour $j \geqslant d$ sont définis par la relation de récurrence $e'_{j+1} = \phi(e'_j)$. $\square$

Proposition 3. *Soient (d, n, a) un triplet comme précédemment. On suppose qu'il existe d' et n' comme précédemment tels que $t = \frac{d}{d'}$ soit un entier et que $\frac{n}{b^d - 1} = \frac{n'}{b^{d'} - 1}$.*

(i) Si σ n'est pas l'identité, on a :

$$D(d,n,a) \simeq D(d',n')^{\oplus \frac{d}{d'}}.$$

(ii) Si σ est l'identité et si t est premier avec p, on a :

$$D(d,n,a) \simeq D(d',n',a'_1) \oplus D(d',n',a'_2) \oplus \cdots \oplus \simeq D(d',n',a'_t)$$

où les a'_i sont les racines t-ièmes de a.

(iii) Si σ est l'identité, $a = 1$ et $t = p$, il existe une suite croissantes de sous-modules de $D(d,n)$ stables par ϕ

$$0 = D_0 \subset D_1 \subset D_2 \subset \cdots \subset D_p = D(d,n)$$

pour laquelle tous les quotients D_m/D_{m-1} ($1 \leqslant m \leqslant p$) sont isomorphes à $D(d',n')$.

Démonstration. Pour tout la preuve, posons $r = \frac{n}{b^d-1} = \frac{n'}{b^{d'}-1}$.

On traite d'abord (i). D'après le lemme 1, on peut supposer $a = 1$. Étant donné que le groupe de Galois absolu de $\mathbb{F}_p$ est un groupe procyclique sans torsion (il est isomorphe à $\hat{\mathbb{Z}}$), ℓ_d est une extension cyclique de degré t de $\ell_{d'}$. On définit pour tout $\alpha \in k$ et $i \in \{0,\dots,d'-1\}$, les éléments suivants de $D(d,n,a)$:

$$f_i(\alpha) = \sum_{s=0}^{t-1} \sigma^{sd'+i}(\alpha)\, u^{-rb^i(b^{sd'}-1)}\, e_{sd'+i}.$$

(On remarquera que l'exposant qui apparaît sur u est un entier étant donné $r(b^{d'}-1) = n'$ en est un.) On vérifie à la main que $\phi(f_i(\alpha)) = f_{i+1}(\alpha)$ pour $i \in \{0,\dots,d'-2\}$, et que $\phi(f_{d'-1}(\alpha)) = u^{n'} f_0(\alpha)$ (la dernière égalité utilise $\sigma^d(\alpha) = \alpha$, ce qui est vrai puisque α est pris dans ℓ_d). Comme par ailleurs, il est clair que à α fixé, la famille des $f_i(\alpha)$ est libre, on en déduit que les sous-objets $F(\alpha) = Kf_0(\alpha) \oplus \cdots \oplus Kf_{d-1}(\alpha)$ sont tous isomorphes à $D(d',n')$. Il suffit donc pour conclure de montrer que t d'entre eux sont en somme directe. Ceci nous amène à chercher des éléments $\alpha_1,\dots,\alpha_t$ tels que chacune des matrices :

$$M_i = \begin{pmatrix} \sigma^i(\alpha_1) & \sigma^i(\alpha_2) & \cdots & \sigma^i(\alpha_t) \\ \sigma^{d'+i}(\alpha_1) & \sigma^{d'+i}(\alpha_2) & \cdots & \sigma^{d'+i}(\alpha_t) \\ \sigma^{2d'+i}(\alpha_1) & \sigma^{2d'+i}(\alpha_2) & \cdots & \sigma^{2d'+i}(\alpha_t) \\ \vdots & \vdots & & \vdots \\ \sigma^{(t-1)d'+i}(\alpha_1) & \sigma^{(t-1)d'+i}(\alpha_2) & \cdots & \sigma^{(t-1)d'+i}(\alpha_t) \end{pmatrix}$$

(pour i variant entre 0 et $d'-1$) soit inversible. En réalité, il suffit pour cela de choisir les α_i de façon à ce que $(a_1,\dots,a_t)$ soit une base de ℓ_d sur $\ell_{d'}$. En effet, on remarque d'abord que $M_i = \sigma^i(M_0)$ et donc qu'il suffit de démontrer l'inversibilité de M_0. On invoque alors le théorème d'Artin d'indépendance linéaire des caractères qui montre que les vecteurs ligne forment une famille libre.

Passons maintenant au (ii) : on suppose donc $\sigma = \mathrm{id}$. On pose cette fois-ci :

$$f_i(\alpha) = \sum_{s=0}^{t-1} \alpha^{t-1-s}\, u^{-rb^i(b^{sd'}-1)}\, e_{sd'+i}$$

pour tout $i \in \{0,\dots,d'-1\}$ et tout $\alpha \in k$. On a encore $\phi(f_i(\alpha)) = f_{i+1}(\alpha)$ pour $i \in \{0,\dots,d'-2\}$, et si α est une racine t-ième de a, on vérifie directement que $\phi(f_{d-1}(\alpha)) = \alpha u^{n'} f_0(\alpha)$. Ainsi, comme il est clair par ailleurs que la famille des $f_i(\alpha)$ ($0 \leqslant i < d'$) est libre, on a $Kf_0(\alpha) + \cdots + Kf_{d-1}(\alpha) \simeq D(d',n',\alpha)$ (toujours sous l'hypothèse $\alpha^t = a$). Si maintenant t est premier à p, a admet t racines t-ièmes distinctes, et un calcul de déterminants de Vandermonde montre facilement que la famille des $(f_i(\alpha))_{0 \leqslant i < d',\, \alpha^t = a}$ est une base de $D(d,n,a)$. La conclusion s'ensuit.

Terminons finalement par la démonstration de l'assertion (iii). Pour tous entiers $i \in \{0,\dots,d'-1\}$ et $j \in \{0,\dots,p-1\}$, on pose :

$$f_{i,j} = \sum_{s=0}^{p-1} s^j\, u^{-rb^i(b^{sd'}-1)}\, e_{sd'+i}$$

et on définit D_m comme le sous-K-espace vectoriel de $D(d,n)$ engendré par les $f_{i,j}$ avec $0 \leqslant i < d'$ et $0 \leqslant j < m$. À nouveau l'utilisation des déterminants de Vandermonde assure la liberté de la famille des $f_{i,j}$, ce qui montre que la dimension de D_m sur K est md'. Par ailleurs, on a les relations $\phi(f_{i,m}) = f_{i+1,m}$ pour $i \in \{0,\dots,d'-2\}$ et :

$$\phi(f_{d-1,m}) = u^{n'} \sum_{\mu=0}^{m} (-1)^{m-\mu} \binom{m}{\mu} f_{0,\mu} \equiv u^{n'} f_{0,m} \pmod{D_{m-1}}.$$

Elles montrent à la fois que D_m est stable par ϕ pour tout m et que les quotients D_m/D_{m-1} sont tous isomorphes à $D(d',n')$. □

La proposition précédente nous conduist à considérer $\mathcal{R}_b$ l'ensemble quotient de $\mathbb{Z}_{(b)}$ (le localisé de $\mathbb{Z}$ en la partie multiplicative des entiers premiers avec b) par la relation d'équivalence :

$$x \sim y \quad \Longleftrightarrow \quad (\exists s \in \mathbb{Z})\ x \equiv b^s y \pmod{\mathbb{Z}}.$$

Via l'écriture en base b, les éléments de $\mathcal{R}_b$ s'interprètent aussi comme l'ensemble des suites périodiques (depuis le début) d'éléments de $\{0,1,\dots,b-1\}$ modulo décalage des indices, où l'on a en outre identifié les suites constantes égale à 0 et à $b-1$.

Soit $r \in \mathcal{R}_d$. Par définition, il est représenté par une fraction (que l'on peut supposer — et que l'on supposera par la suite — irréductible) $\frac{s}{t}$ où t est un nombre premier avec b. On vérifie directement que l'ordre de b modulo t ne dépend pas du représentant (irréductible) choisi : on l'appelle la *longueur* de r et on le note $\ell(r)$. On pourra remarquer qu'à travers le point de vue « suites périodiques », $\ell(r)$ s'interprète simplement comme la plus petite période.

Notons $\mathcal{N}(r)$ l'ensemble des entiers relatifs n pour lesquels $\frac{n}{b^{\ell(r)}-1}$ est un représentant de r. La définition de $\ell(r)$ implique immédiatement la non-vacuité de $\mathcal{N}(r)$. Le lemme 2 montre que les objets $D(\ell(r),n)$ pour n variant dans $\mathcal{N}(r)$ sont isomorphes entre eux. Notons $D(r)$ l'un de ces objets. Si en outre $\sigma = \mathrm{id}$, le même lemme 2 permet de définir $D(r,a)$ pour tout $a \in k^\star$ comme l'un des ϕ-modules $D(\ell(r),n,a)$, $n \in \mathcal{N}(r)$.

Théorème 4. *Les $D(r)$ (resp. $D(r,a)$ si $\sigma = \mathrm{id}$) sont des objets simples de $\mathrm{Mod}^{\phi}_{/K}$. De plus, ils sont deux à deux non isomorphes.*

Démonstration. Pour simplifier la preuve, on suppose dans la suite $a = 1$, laissant au lecteur l'exercice (facile) d'adapter les arguments au cas général.

Notons $\ell = \ell(r)$ et considérons n tel que $\frac{n}{p^\ell - 1}$ représente r. Soit D un sous-objet non nul de $D(r)$, et soit $x = \lambda_1 e_1 + \cdots + \lambda_\ell e_\ell$ un élément non nul de D pour lequel le nombre de λ_i non nuls est minimal. Quitte à remplacer x par $\phi^m(x)$ et pour un certain entier m, on peut supposer $\lambda_1 \neq 0$. Quitte à renormaliser x, on peut en outre supposer $\lambda_1 = 1$. On a alors :

$$\phi^d(x) - u^n x = \sum_{i=2}^{\ell} (\phi^d(\lambda_i) u^{b^i n} - \lambda_i u^n) e_i \in D.$$

Supposons par l'absurde qu'il existe un indice $i > 1$ tel que $\lambda_i \neq 0$. Montrons dans un premier temps que $\phi^d(\lambda_i) u^{b^i n} \neq \lambda_i u^n$. Encore par l'absurde : si ce n'était pas le cas, on déduirait $\frac{\phi^d(\lambda_i)}{\lambda_i} = u^{-n(b^i-1)}$ et puis $v(b^d-1) = -n(b^i-1)$ où v est la valuation u-adique de λ_i. Ainsi, on aurait $r = \frac{-v}{b^i-1}$, et on obtiendrait une contradiction avec la définition de ℓ. Au final, $\phi^d(\lambda_i) u^{b^i n} \neq \lambda_i u^n$, et l'élément $\phi^d(x)$ est un élément non nul de D qui, sur la base des (e_i), a strictement moins de coefficients non nuls que n'en avait x. Ceci contredit la minimalité supposée et montre que $x = e_1$. On en déduit e_1 est élément de D et, puisque ce dernier est par hypothèse stable par ϕ, il contient nécessairement tous les e_i. En conclusion, $D = D(r)$ et le théorème est démontré.

Pour prouver que $D(r)$ n'est pas isomorphe à $D(r')$, il suffit de remarquer que $\ell(r)$ et $\mathcal{N}(r)$ se retrouvent tous deux à partir de $D(r)$: le premier en est la dimension, alors que le second est l'ensemble des entiers n pour lesquels il existe un $x \in D(r)$ non nul vérifiant $\phi^{\ell(r)}(x) = u^n x$. Finalement, il est clair qu'à partir de ces deux données, r est entièrement déterminé dans le quotient $\mathcal{R}_b$. □

Classification des objets simples

Nous souhaitons désormais montrer la réciproque du théorème 4, c'est-à-dire que les objets simples de $\mathrm{Mod}^{\phi}_{/K}$ sont tous isomorphes à un certain $D(r)$ (ou $D(r,a)$ si $\sigma = \mathrm{id}$). Pour cela, nous considérons D un objet simple de $\mathrm{Mod}^{\phi}_{/K}$, $(e_1, \dots, e_d)$ une base de D et G la matrice de ϕ dans cette base, *i.e.* l'unique matrice vérifiant l'égalité :

$$(\phi(e_1), \dots, \phi(e_d)) = (e_1, \dots, e_d)G.$$

On rappelle, à ce propos, la formule de changement de base qui interviendra plusieurs fois dans la suite : si $\mathcal{B}' = (e'_1, \dots, e'_d)$ est une autre base de D et si P est la matrice de passage de $(e_1, \dots, e_d)$ à $\mathcal{B}'$, alors la matrice de ϕ dans la base $\mathcal{B}$ est donnée par la formule $P^{-1}G\phi(P)$. Il résulte de cette formule que, quitte à multiplier les e_i par une certaine puissance de u, on peut supposer que G est à coefficients dans $k[[u]]$. En réalité on aura besoin d'un résultat un peu plus précis, conséquence du lemme suivant. Introduisons avant tout une dernière notation : soit γ la valuation u-adique de $\det G$.

Lemme 5. *Soit N un entier strictement supérieur à $\frac{p\gamma}{b-1}$ et H une matrice à coefficients dans $k[[u]]$ congrue à G modulo u^N. Alors, il existe une matrice P à coefficients dans $k[[u]]$ et inversible dans cet anneau telle que $PG\phi(P)^{-1} = H$.*

Démonstration. On définit une suite de matrices (P_i) (*a priori* à coefficients dans K) par $P_0 = I$ et la formule de récurrence $P_{i+1} = H\phi(P)G^{-1}$. On a directement $P_1 = HG^{-1}$ d'où on déduit, en utilisant l'hypothèse de l'énoncé, que $P_1 \equiv I \pmod{u^{N-v}}$, *i.e.* $P_1 - P_0$ est divisible par u^{N-v}. Par ailleurs, pour tout $i \geqslant 1$, on a $P_{i+1} - P_i = H\phi(P_i - P_{i-1})G^{-1}$, d'où il suit que si $P_i - P_{i-1}$ est divisible par u^v, alors $P_{i+1} - P_i$ est divisible $u^{pv-\gamma}$. Une récurrence immédiate montre alors que $P_{i+1} - P_i$ est divisible par u^{v_i} où la suite (v_i) est définie par $v_0 = N - \gamma$ et $v_{i+1} = bv_i - \gamma$. De $v_0 > \frac{\gamma}{b-1}$, on déduit que (v_i) est une suite croissante qui tend vers l'infini. Ainsi $P_{i+1} - P_i$ converge vers 0 pour la topologie u-adique, et la suite des (P_i) converge vers une matrice P. Celle-ci vérifie $PG\phi(P)^{-1} = H$ et est congrue à l'identité modulo u du fait que chacun des v_i est strictement positif. Elle est donc inversible dans $k[[u]]$, comme demandé. □

Le lemme nous assure que, quitte à modifier la base $(e_1, \dots, e_d)$, on peut remplacer G par une matrice qui lui est congrue modulo u^N. En particulier, on peut supposer que G a tous ses coefficients dans $\mathbb{F}_q[[u]]$ pour un certain q. C'est ce que nous ferons par la suite.

Soit M le sous-$\mathbb{F}_q[[u]]$-module de D engendré par les e_i ; il est libre de rang d. On définit deux suites récurrentes (x_i) et (n_i) comme suit. On pose en premier lieu $x_0 = e_1$. Maintenant, si x_i est construit, on définit n_i comme le plus petit entier tel que $\phi(x_i) \in u^{n_i}M$ et $x_{i+1} = u^{-n_i}x_i$. On remarque tout de suite que tous les x_i sont des éléments de M qui ne sont pas dans uM.

Lemme 6. *Pour tout i, on a $n_i \leqslant \gamma$.*

Démonstration. Il suffit de montrer que si $x \in M$, $x \notin uM$ alors $\phi(x) \notin u^{\gamma+1}M$. Or, le prémisse entraîne l'existence d'une $k[[u]]$-base $(x_1, \dots, x_d)$ de M avec $x_1 = x$. Si P est la matrice de passage de $(e_1, \dots, e_d)$ à $(x_1, \dots, x_d)$ la matrice du ϕ dans la base $(x_1, \dots, x_d)$ est donnée par la formule $H = P^{-1}G\phi(P)$. Comme P est inversible dans $k[[u]]$, son déterminant a une valuation u-adique nulle, d'où on déduit que le déterminant de H a pour valuation u-adique γ. Ainsi, sa première colonne ne peut pas être multiple de $u^{\gamma+1}$ ce qui correspond exactement à ce que l'on voulait. □

Soit c un entier strictement supérieur à $\frac{\gamma}{b-1}$. Notons $\bar{x}_i$ la réduction modulo u^c de x_i : c'est un élément de l'ensemble *fini* M/u^cM. D'après le principe des tiroirs, il existe deux indices $i < j$ tels que $\bar{x}_i = \bar{x}_j$. Posons $\delta = j - i$ et $x = x_i$. En déroulant les définitions, on obtient :

$$\phi^{\delta}(x) \equiv u^n x \pmod{u^{n+c}M}$$

avec :

$$n = b^{\delta-1}n_i + b^{\delta-2}n_{i+1} + \cdots + bn_{j-2} + n_{j-1}.$$

Nous souhaitons à présent relever la dernière congruence en une vraie égalité dans M. Pour cela, on commence par écrire $\phi^{\delta}(x) = u^n(x + u^c y)$ et on définit une nouvelle suite récurrente (z_i) par

$z_0 = x$ et $z_{i+1} = u^{-n}\phi^\delta(z_i)$. On a $z_1 - z_0 = u^c y$ et $z_{i+1} - z_i = u^{-n}\phi^\delta(z_i - z_{i-1})$. Il s'ensuit que $z_{i+1} - z_i$ est un multiple de u^{v_i} où (v_i) est la suite récurrente définie par $v_0 = c$ et $v_{i+1} = b^\delta v_i - n$. Maintenant, le lemme 6 donne :

$$n \leqslant \gamma(b^{\delta-1} + b^{\delta-2} + \cdots + 1) = \gamma\,\frac{b^\delta - 1}{b-1} < c(b^\delta - 1)$$

à partir de quoi on déduit $\lim_{i\to\infty} v_i = +\infty$. Ainsi la suite (z_i) converge vers un élément $z \in M$ (car tous les v_i sont positifs) vérifiant $\phi^\delta(z) = z$. Par ailleurs, on a $z \equiv x \pmod u$, ce qui assure qu'il est non nul. On a donc montré le résultat intermédiaire important suivant :

Théorème 7. *Soit D un objet simple de $\mathrm{Mod}^\phi_{/K}$. Alors, il existe des entiers $\delta > 0$, $n \geqslant 0$ et un élément non nul $z \in D$ tels que $\phi^\delta(z) = u^n z$.*

Corollaire 8. *Soit D un objet simple de $\mathrm{Mod}^\phi_{/K}$.*
- *Si σ n'est pas l'identité, il existe $r \in \mathcal{R}_b$ tel que $D \simeq D(r)$.*
- *Si σ est l'identité, il existe $r \in \mathcal{R}_b$ et $a \in k^\star$ tels que $D \simeq D(r,a)$.*

Démonstration. D'après le théorème 7, il existe des entiers $\delta > 0$, $n \geqslant 0$ et un morphisme (dans $\mathrm{Mod}^\phi_{/K}$) non nul $f : D(\delta,n) \to D$. La simplicité de D assure que f est surjectif, et donc que D se retrouve parmi les constituants de Jordan-Hölder de $D(\delta,n)$. Écrivons la fraction $r = \frac{n}{b^\delta - 1}$ sous la forme $\frac{m}{b^{\ell(r)}-1}$. Le quotient $\frac{\delta}{\ell(r)}$ est alors un nombre entier.

Si σ n'est pas l'identité, la proposition 3.(i) montre que $D(\delta,n)$ s'écrit comme une somme directe de copies de $D(r)$. En particulier, puisque les $D(r)$ sont simples d'après le théorème 4, tous les quotients de Jordan-Hölder de $D(\delta,n)$ sont isomorphes à $D(r)$, et le théorème est démontré dans ce cas. Supposons maintenant qu'au contraire $\sigma = \mathrm{id}$. On écrit $\frac{\delta}{\ell(r)} = p^v t$ où t est un entier premier à p. Plusieurs applications successibles de la proposition 3.(iii) montrent que $D(\delta,n)$ admet une suite de composition dont les quotients successifs sont tous isomorphes à $D(\delta p^{-v}, n')$ pour un certain entier n'. L'alinéa (ii) de la même proposition montre alors que les constituants de Jordan-Hölder sont dans ce cas tous isomorphes à des $D(r,a)$ pour certains éléments a de $k^\star$ (qui peuvent varier d'un composant à l'autre). La conclusion en découle. $\square$

Références

[1] E. Hellmann, *On the structure of some moduli spaces of finite flat group schemes*, preprint